練馬区
委託事業者等向け情報セキュリティ教材
（共通編）

令和８年度用

企画部　情報政策課

はじめに

- 委託事業者等の皆様は、受託業務の遂行にあたり、区と同等以上の情報セキュリティ対策を実施する必要があります。
- 本研修教材は、「特記事項」が添付された契約等において、皆様に遵守していただく情報セキュリティ対策（主に特記事項の内容）をまとめたものです。
- 本教材は、**主に委託事業者を想定して作成しています**。
  指定管理者や派遣契約、リース会社においては、適宜文言を置き換えてご活用ください。

用語の定義

■ 本教材で使用する用語の定義を以下に示します。

委託事業者等	委託事業者および指定管理者
区	練馬区
情報	委託契約の受託者が、委託者から受託した業務を履行するにあたり、委託契約で取り扱う情報
特記事項	情報の取扱いルールについて記載し、契約等に際し仕様書に添付する以下の書類 • 情報の保護および管理に関する特記事項 • 指定管理における情報の保護および管理に関する特記事項 • 労働者派遣契約における情報の保護および管理に関する特記事項 • メンテナンスリースにおける情報の保護および管理に関する特記事項 • ファイナンスリースにおける情報の保護および管理に関する特記事項 • 特定個人情報の保護および管理に関する特記事項（４種類）

情報の保護および管理に関する特記事項とは

「情報の保護および管理に関する特記事項」について、基本的な内容を以下にまとめます。

- **情報の保護および管理に関する特記事項とは**
  委託事業者等が、個人情報をはじめとする区の情報を取り扱う業務に関して共通に遵守すべき基本的な事項を規定したものです。

- **特記事項の目的**
  契約等における個人情報の保護、および一定の情報セキュリティ水準を確保することを目的としています。
  契約書に特記事項を添付することで、区が求める個人情報の保護および情報セキュリティレベルを明らかにしています。

- **記載内容の概要**
  対象は当該契約で取り扱う情報（区の情報）であり、個人情報だけではありません。
  情報の取扱いルールとして、「受託業務の従事者へのセキュリティ教育実施・報告の義務」や「情報の管理における義務」などを規定しています。

本教材が対象とする契約等について

- 本教材は、特記事項が添付されている契約等を対象にしています。そのうち、**「特定個人情報の保護および管理に関する特記事項」**が添付されている契約等は、本教材と併せて、**「練馬区委託事業者等向け情報セキュリティ教材（特定個人情報編）」**（以下「特定個人情報の教材」という。）も活用し、研修を実施してください。

- 特定個人情報（マイナンバーを含む個人情報）を取り扱う場合は、**より厳重なルールが決められています**。「特定個人情報の教材」で確認してください。

特

「特定個人情報の教材」を確認する必要があるページは、右上に左図のような表記をしています。
※カッコ書きのページ番号は、参照する特定個人情報の教材のページ番号を示しています。

教材の利用イメージ

本教材(共通編) 特(P.３)

○○に係る遵守事項

1　×××をすること。
2　△△△をすること。
3　■■■をしないこと。

- 5 -

「特」表記があるページ（項目）は「特定個人情報の教材」を併せて確認する。

※ 特定個人情報を取り扱う契約等

委託事業者向けの教材（特定個人情報編） 委(P.5)

○○に係る遵守事項

A　◇◇◇をすること。
B　◎◎◎をしないこと。

- 3 -

左のイメージ図の場合、１～３の３項目とA･Bの２項目の合計５項目を遵守する必要があります。

本教材の目的

- 区では、委託業務における情報セキュリティを確保し、情報漏えい等の事故を防止するため、契約書に「特記事項」を添付しています。

- 本教材は、受託者および受託業務の従事者に対し、それぞれの立場から「特記事項」の内容を正しく理解し、遵守していただくことを目的としています。

- 本教材の構成／主な想定対象

本教材の構成	主な想定対象		
	受託者	管理責任者	従事者
第１章 契約の前提となる事項	○	―	―
第２章 契約締結時に実施すべき事項	○	―	―
第３章 履行中に実施すべき事項	○	○	○
第４章 契約終了時に実施すべき事項	○	―	―
第５章 再委託について	―	○	○

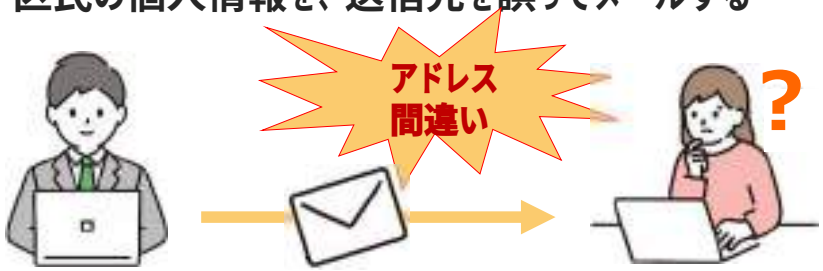
第３章は管理責任者を含めた従事者の遵守事項も記載しているため、情報セキュリティ教育に使用してください。
また、巻末の復習テストを適宜活用してください。

情報セキュリティ事故等とは

■ 「情報セキュリティ事故等」とは、以下のような事象またはそれらのおそれ・兆候を言います。

情報漏えい

例：区民の個人情報を、送信先を誤ってメールする



不正アクセス

例：他人のID・パスワードを使って、権限の無いシステムにログインする

ウイルス感染

例：パソコンがウィルスに感染する

情報資産の紛失・盗難

例：自転車のカゴに入れておいた書類が盗まれる

情報資産の所在不明

例：情報機器の管理が不十分で所在不明になる

その他、特記事項や関係法令等への違反

例：私物のパソコンやスマートフォンを業務で利用する

委託事業者等における情報漏えいの事例

【横須賀市】健診結果票に別人情報、結果や既往症など記載（令和6年12月）

- 神奈川県横須賀市は、国保特定健康診査において一部受診者に別人の健診結果を送付していたことを明らかにした。
- 同市によれば、令和６年12月20日、委託業者が約1300人宛てに送付した健診結果票のうち**101人分について、別人の健診結果が印刷されていた**ことが判明したもの。
- データから**印刷を行った際に不手際があり、表面と裏面に別人の情報を印刷**してしまったという。氏名や生年月日、性別、年齢、既往歴、服薬状況、自覚症状、3年分の健康診査結果などが含まれる。
- 同市では対象者に速達郵便で謝罪を実施。同月24日以降、対象者を訪問して謝罪するとともに、誤った結果票の回収を行っている。

（出典：https ://www.security-next.com/165816）

「特記事項」は、このような事故や情報の不適切な取扱いの発生を未然に防止するために、**①契約締結当初、②履行中、③契約終了時**の各段階で、受託事業者等が情報を適切に管理することを目的としています。

第１章　契約の前提となる事項

対象：受託者

本章は、受託者が区の業務を受託する前提として
守るべき事項を記載しています。

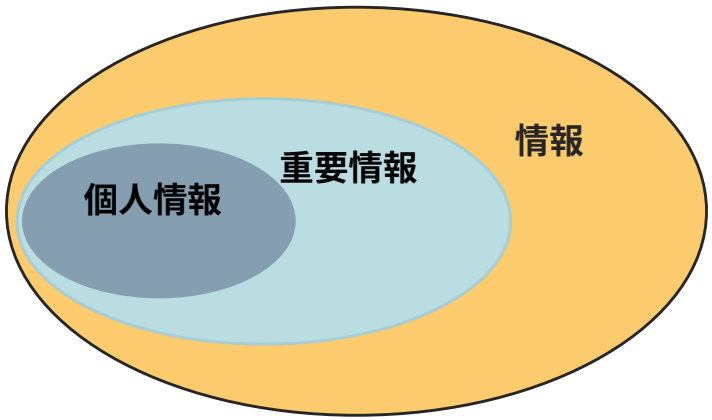
契約の前提となる事項（１／２）

特(P.8,9)

ａ．重要情報とは

個人情報や**その情報が脅威にさらされることにより区政運営に重大な影響を及ぼす情報**をいいます。
受託業務を遂行するにあたっては、**どのような重要情報をどのように扱うのかを特定**した上で、特記事項に基づき重要情報を厳重に取り扱う必要があります。

重要情報とその取扱いの例



区の情報システムを使用する。
例：住民情報システム

受け取った情報を自社内で取り扱う。
例：自社のパソコン、サーバ

区民の個人情報を含むファイル
（例：名簿、連絡先一覧表）

・氏名
・住所
・電話番号
・・・

申請書・届出書

・申請者
・申請内容
・承認者
・・・

公開前の計画書　等

・件名
・目的
・実施期間
・・・

契約の前提となる事項（２／２）

特(P.10)

ｂ．個人情報等の重要情報を守るために

個人情報とは、生存する個人に関する情報であって、以下のいずれかに該当するものをいいます。

①当該情報に含まれる氏名、生年月日その他の記述等（個人識別符号（※）を除く。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

②個人識別符号が含まれるもの　【個人情報の保護に関する法律第２条】

※ その情報単体から特定の個人を識別することができるものとして政令で定められた文字、番号、記号その他の符号のこと。

区は、特記事項の記載内容と同等以上の情報セキュリティ対策を実施している（実施することができる）事業者にのみ、区の業務を委託することができます。そのため、区では個人情報を取り扱う契約について、契約締結前に「安全管理体制確認書」を提出（※）することを求めています。

また、業務を受託しようとする事業者は、情報を保護し、適切に管理するために、自社における個人情報保護方針や、情報セキュリティに関する規程、運用マニュアルといった情報管理ルールを定め、従事者に周知・徹底する必要があります。

※ 提出にあたり、件名、契約期間、受託事業者名等が契約書の記載と一致していることをチェックしてください。

区の情報セキュリティレベル ≦ 受託者の情報セキュリティレベル

区の情報を取り扱う受託者は、特記事項と同等以上の情報セキュリティレベルを維持する必要がある。

第２章　契約締結当初に実施すべき事項

対象：受託者

本章は、受託者が契約締結当初に実施すべき事項を記載しています。

契約締結当初に実施すべき事項（１／３）

特(P.12)

ａ．管理体制の確立

情報セキュリティ事故等を防止するためには、適切な情報の管理が必須であり、受託業務における**体制を明確にする**ことが大前提です。

そのため、受託者は**個人情報を取り扱う契約の場合、**情報の管理に責任を持つ**「管理責任者」を任命**し、また、受託業務に従事する**「従事者」を特定**して体制を明確にし、区に**書面で報告する**必要があります。

報告内容に変更があった場合は、**速やかに再報告（再提出）する**必要があります。

しなければならないこと

※　書面の参考様式は、区から提示します。

個人情報を取り扱う契約の場合

・管理責任者について、「情報の管理責任者選任届」を**書面で提出する**。
・従事者について、「受託業務従事者報告書」を**書面で提出する**。
・提出にあたり、会社名、契約件名等が**契約書と一致しているかチェックする**。

契約締結当初に実施すべき事項（２／３）

ｂ．情報セキュリティ教育

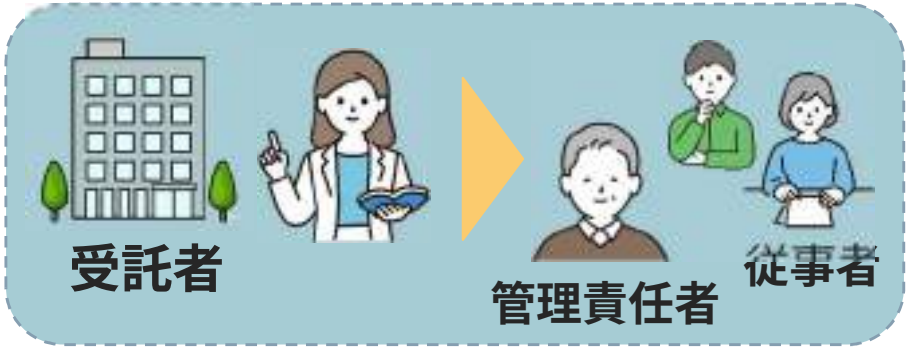
受託者は特記事項の内容を周知徹底するために、**個人情報を取り扱う契約の場合は、管理責任者も含めた従事者に対する情報セキュリティ教育**を実施して、その結果を区に**書面で報告する**必要があります。

また、区が特記事項の遵守に必要な教育を実施する時は、管理責任者および従事者に教育を受けさせる必要があります。

管理責任者および従事者に変更があった場合は、**速やかに教育を実施し、再報告（再提出）する**必要があります。

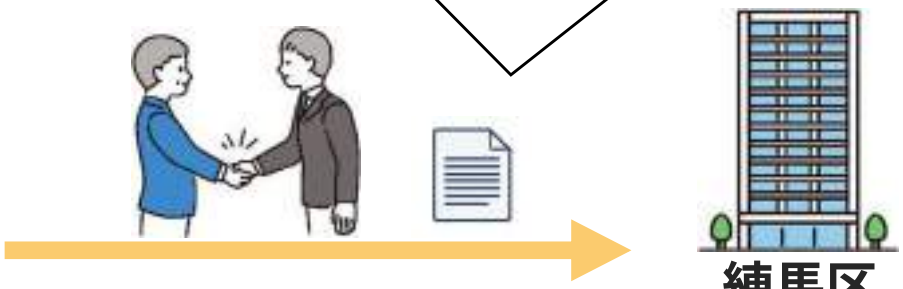
しなければならないこと

管理責任者および従事者に対し、**情報セキュリティ教育を実施**



※ 書面の参考様式は、区から提示します。

個人情報を取り扱う契約の場合	教育の実施状況について、「情報セキュリティ教育実施結果報告書」を**書面で提出する**。その際は、会社名、受託業務件名が**契約書と一致しているかチェックする**。



契約締結当初に提出する書類について

- 個人情報を取り扱う契約等では、契約締結の際に以下の書類を提出する必要があります。提出にあたり、以下の項目を**必ず**チェックしてください。

提出する書類とチェック内容

情報の管理責任者選任届

- □ 件名、契約期間、受託事業者名等は契約書の記載と一致していますか？
- □ 管理責任者の役職と氏名は記載されていますか？

受託業務従事者報告書

- □ 会社名、契約件名は契約書の記載と一致していますか？
- □ 管理責任者氏名は「情報の管理責任者選任届」の氏名と一致していますか？
- □ 従事者氏名は実際に業務している者と一致していますか？

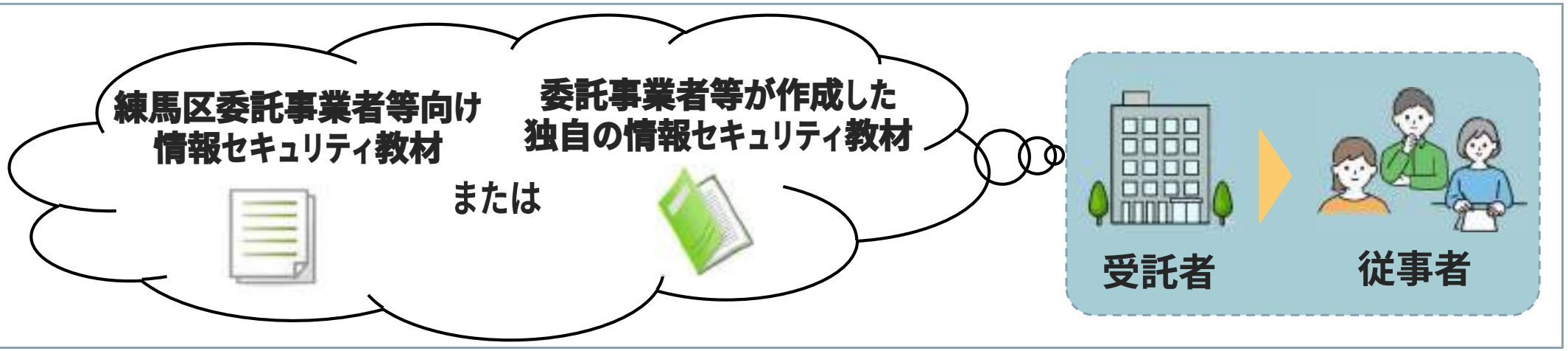
情報セキュリティ教育実施結果報告書

- □ 会社名、受託業務件名は契約書の記載と一致していますか？
- □ 管理責任者氏名は「情報の管理責任者選任届」の氏名と一致していますか？
- □ 参加人数および配付人数の合計は、「受託業務従事者報告書」の従事者数と一致していますか？

※ 特定個人情報を取り扱う契約等では、上記に追加して提出する書類があります。「特定個人情報の教材」で確認してください。

情報セキュリティ監査では、ここを指摘しました！

従事者の情報セキュリティ教育結果報告書を提出していない事業者がいました。



個人情報を取り扱う契約では、
従事者の全員に情報セキュリティ教育を実施し、
区に書面で報告してください。

- 情報セキュリティに関する知識と意識が十分でないまま受託業務に従事していた場合、情報セキュリティ事故等の発生リスクが高まります。
- 契約期間中に追加となった従事者に対しても、速やかに教育を実施し、区に書面で報告してください。

契約締結当初に実施すべき事項（３／３）

ｃ．緊急時対応の手順化

情報セキュリティ事故や災害等発生時に備えた緊急時対応手順を策定し、**管理責任者を含めた従事者に周知する**必要があります。これは、事故や災害等によって情報が脅威にさらされても、可能な限り早く対応して、影響を最小限に抑えられるようにするためです。

また、緊急時対応手順の実効性を高めるために、**定期的な確認または訓練を実施する**必要があります。

遵守事項のイメージ

● 管理責任者を含めた従事者に対し、緊急時対応手順を周知

● 緊急時対応手順に基づき迅速に対応

第３章　履行中に遵守すべき事項

対象：受託者、管理責任者、従事者

本章は、受託業務に従事する方が業務を遂行する際に守っていただきたいことを記載しています。
管理責任者を含めた従事者向け研修資料として適宜活用してください（教材の最後に復習テストもあります）。

履行中に遵守すべき情報セキュリティルールの重要性

情報セキュリティルールの重要性

- 皆さんは、業務の中で多くの情報（印刷した帳票、電子データおよび電子データを格納した記録媒体等）を取り扱っています。その中には、区民の情報をはじめとする重要な情報が含まれている可能性があるため、**情報セキュリティルールに従い作業することが重要**になります。それにより、重大な情報セキュリティ事故等が起きにくくなります。

➢ 情報セキュリティ事故等とは…

- 情報セキュリティ事故等の発生を防ぐため、区の業務に従事する皆さんに守っていただきたい、情報セキュリティ上の**16のルール**について取り上げます。

履行中に遵守すべき事項（１／16）

（１）守秘義務等

【情報を取り扱う際の遵守事項】

１）個人の権利利益を侵害することのないよう、情報を適正に取り扱う。

２）個人情報を収集する時は、受託業務の履行を達成するために必要な範囲内で、適法かつ公正な手段により行う。

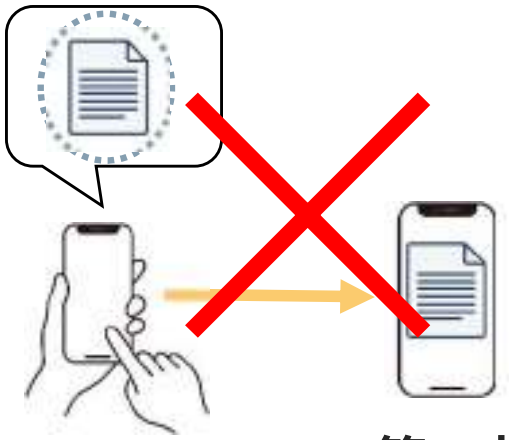
３）受託業務の履行にあたり、知り得た情報を第三者に漏らさない。

４）情報を第三者に提供しない。

５）情報を他の用途に使用しない（ソーシャルメディアへの発信を含む）。

遵守事項のイメージ

● 情報を漏らさない･提供しない



第三者

第三者

● 情報を他の用途に使用しない

ソーシャルメディアへの発信

他の用途

例えば、こんな事故が起きています。

【堺市】元職員が外部へ個人情報の一部を流出 堺市文化振興財団（令和７年９月）

- 堺市の公益財団法人の元職員で、財団が舞台管理運営業務を委託している業者の従業員（以下、元職員）が、財団の管理する予約サービス会員等の個人情報37,164名分を含むデータを窃取し、SNSを通じて、財団および財団職員に対する誹謗中傷をする事案が発生した。
- 原因として、データが窃取された時点において、個人データにパスワードを設定していなかったため閲覧が可能であった。かつ、外部記録媒体の使用に関する制限が十分に講じられておらず、情報の持ち出しが可能な環境であった。
- 再発防止に向けた対応として、個人情報データへのアクセスを制限し、データにパスワードを設定する。アクセスログを監視し、外部記録媒体の使用を制限。職員向けセキュリティ・コンプライアンス研修を実施する。電話、ファックスおよびメールによる、予約サービス会員専用の相談窓口を設置する。

（出典： https://www.sakai-bunshin.com/wp-content/uploads/2025/09/報道提供.pdf ）

履行中に遵守すべき事項（２／16）

特(P.15)

（２）情報の郵送

【記録媒体（※）の郵送時の遵守事項】 ※ 情報システム機器のハードディスクを含む。

１）情報を格納する時は、ファイルに**パスワードを設定する等によりデータを暗号化する**。

２）重要情報を格納する時は、**中身の入れ違いがないか確認**し、**追跡可能な移送手段**を用いる。

３）情報の格納の有無に係わらず、**郵送の記録を管理簿により管理**する。

【参考】 記録媒体郵送時の取扱い

	パスワード	追跡移送	管理簿
情報	○	×	○
重要情報	○	○	○
情報なし	×	×	○

凡例 ○：要対応 ×：対応不要

【印刷物･文書の郵送時の遵守事項】

重要情報を郵送する時は、中身の入れ違いや宛先に誤りがないか確認し、**特定記録郵便または親展表示で送付**する。

遵守事項のイメージ

記録媒体の郵送

パスワード設定等により暗号化を行う

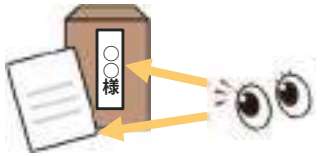
追跡可能な移送手段を用いる

○簡易書留 ○特定記録郵便

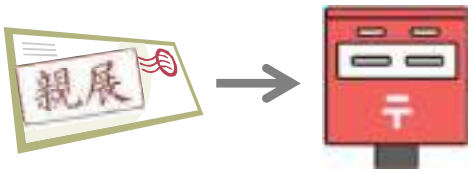
管理簿に記録する

印刷物･文書の郵送

入れ違いや宛先誤りがないか確認する



特定記録郵便または親展表示で送る

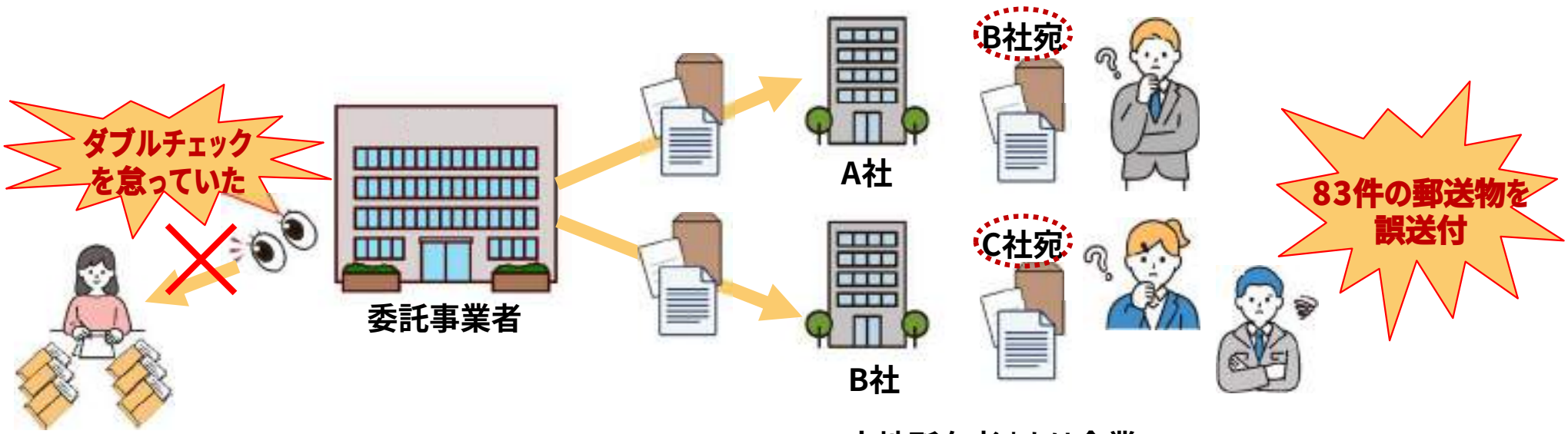


例えば、こんな事故が起きています。

【神奈川県】委託事業者が郵送物を誤送付（令和7年7月）

- 土砂災害防止法の基礎調査業務を受注した委託事業者が、土地所有者あての郵便物83件の「氏名」と「住所」を誤った組み合わせで送付した。　郵送先の企業から宛名の誤りについて情報提供があり、委託事業者に作業内容の確認を求めたところ、**83件の誤送付**が判明した。
- 委託事業者が、県が貸与した地権者情報（Excelファイル等）を用いて宛名ラベルを作成した際、**「宛名」と「住所」を誤った組合せで印刷し、確認せず発送**したため事故が発生した。
- 再発防止策として、データの取り扱いに細心の注意を払うことや、発送する前のダブルチェックの徹底など、適切な事務処理を委託事業者に求めた。

（出典： https://www.pref.kanagawa.jp/docs/wk7/prs/r0114062.html）



情報セキュリティ監査では、ここを指摘しました！

重要情報を含む文書を、特定記録郵便または親展表示で送っていない事業者がいました。

重要情報を含む文書を郵送する時は、
特定記録郵便または親展表示が必要です。

さらに、**記録の管理**（送付の記録）を実施すると、事故等発生時に原因や被害状況を速やかに把握し、迅速な対応をとることができます。**発送件数が多い等、都度の記録が難しい場合を除き、原則として送付の記録は残す**ようにしてください。

履行中に遵守すべき事項（３／16）

特(P.16)

（３）情報の送信（メール･FAX）

【送信時の遵守事項】
１）重要情報をメールで送信する時は、メール本文には記載せず添付ファイルとし、ファイルにパスワードを設定する等によりデータの暗号化を行う。
２）情報をメールやFAXで送信する時は、宛先および添付ファイルを誤らないように十分注意する。

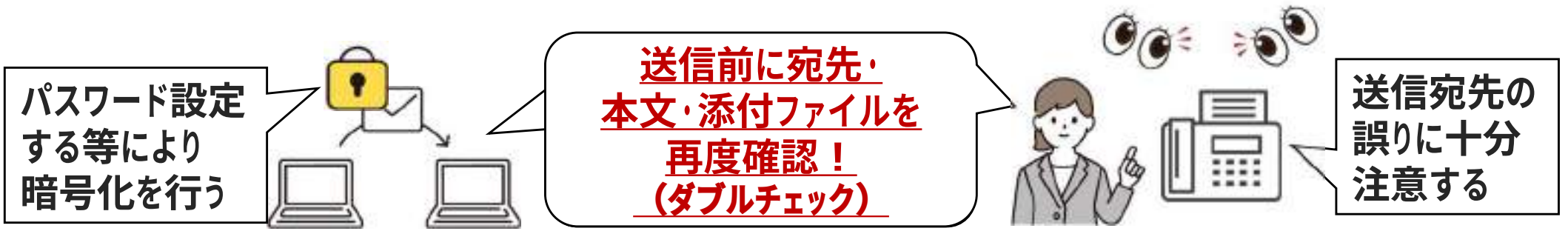
遵守事項のイメージ

メール送信

- 重要情報はメール本文に記載しない
- パスワードを設定する等により添付ファイルを暗号化する
- 送信宛先および添付するファイルに十分注意する

FAX送信

- 送信宛先、送信内容に注意する



※ パスワードはメール以外の方法で送信先に伝える手段を整備（例：あらかじめ相手先と設定するパスワードを決めておく）すると、一層有効な対策となります。
※ セキュリティが確保されたファイル送信サービスの利用も有効です（個人で契約しているサービスの利用はNG）。

履行中に遵守すべき事項（４／16）

（４）メールの利用

【メール送信時の遵守事項】
区民等のメールアドレスも個人情報であるため、複数の区民等にメールを送る際には、TOやCCではなく、**BCCを利用して**個人情報が漏れないようにする。

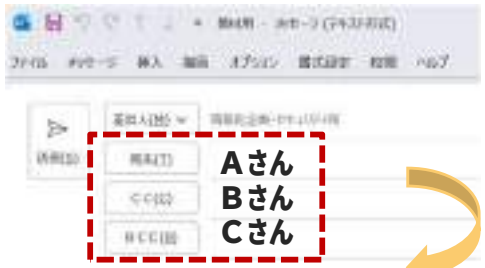
【メール受信時の遵守事項】
不審なメール（心当たりのないメール等）は、組織内部の情報を狙った「標的型攻撃メール」の可能性があるため、添付ファイルを開く前に、メール本文や差出人等に不審な点がないかを確認する。**安全が確認できるまでは添付ファイルやメール本文のURLを開かない。**

遵守事項のイメージ

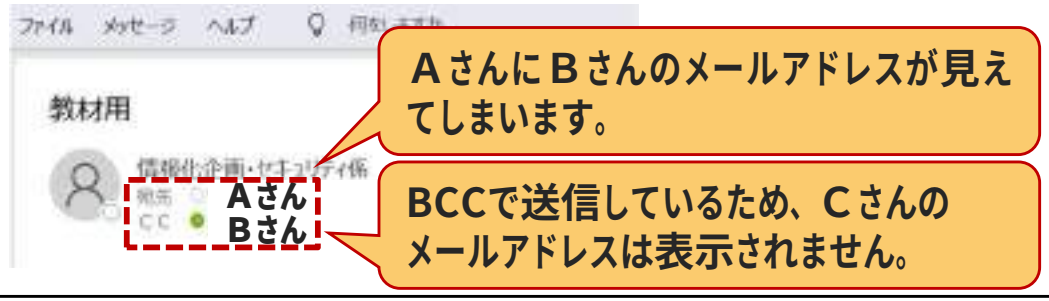
メールを同時に複数の区民等に送信する場合は、メールアドレスを**BCCに設定**する。

宛先設定によるメールアドレスの見え方の違い
TO：送った人全員から見える
CC：送った人全員から見える
BCC：**他の人から見えない**

TO、CC、BCCをこのように設定すると



受信者にはこのようなメールが届きます。



履行中に遵守すべき事項（４／16）

遵守事項のイメージ（つづき）

不審なメールを受信した場合は、**正当性が確認できるまでは、添付ファイルを開いたり、メール本文のURLをクリックしない**ようにします。

不審メールの特徴例（判別のための着眼点）

□ **メールの差出人**
- 差出人のメールアドレスと署名（メール本文の一番下に記載されている差出人情報）のメールアドレスが異なる　等

□ **添付ファイル**
- 実行形式ファイル（exe / scr / cpl等）が添付されている
- ショートカットファイルが添付されている（lnk等）　等

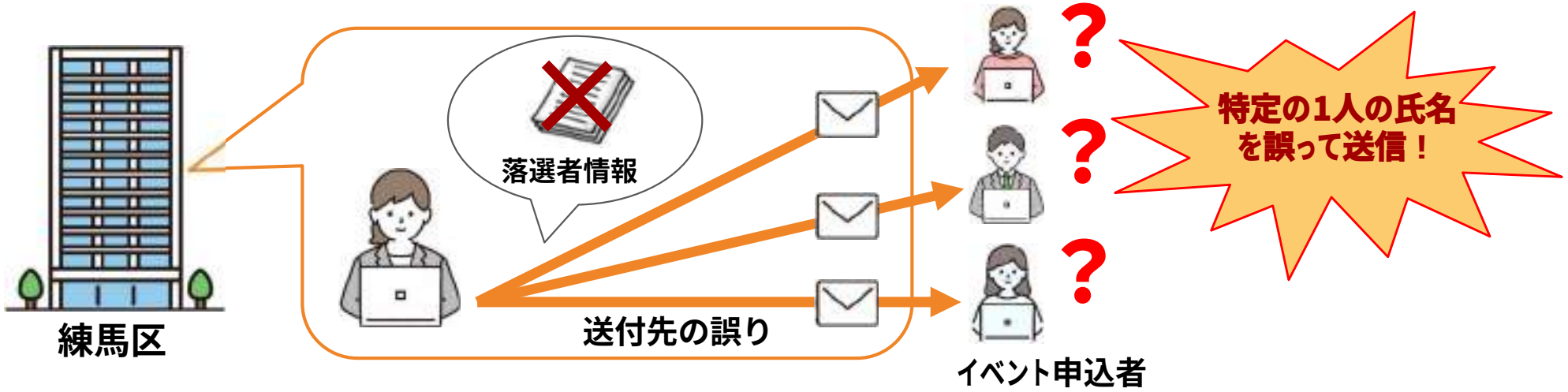
□ **メールのテーマ、内容**
- 区民からのクレームを装い、メール本文のURLや添付ファイルを開かせようとする
- 公的機関によるセキュリティの注意喚起を装い、添付ファイルを開かせようとする
- システム管理者を装い、IDやパスワードの入力を要求する
- 文法や仮名遣いがでたらめである
- 正常に表示できない文字（繁体字、簡体字）がある　等

上記の特徴例に該当しない標的型攻撃メールもあります。
被害に遭わないために、**受信したメールに不審な点がないかを、注意して見極める**ように心がけてください。

例えば、こんな事故が起きています。

【練馬区】イベントのキャンセル受付メールの誤送信　（令和６年６月）

- 指定管理者の職員が、イベントの申込者に対し、当落結果をメールで送信した。その後当選者4名からキャンセルのメールが届いたため、担当者がキャンセル受付メールを4名に対して送信した。次の日、キャンセルを申し出ていない方から、他人宛のキャンセル受付メールが届いたと問い合わせがあり、誤送信が判明した。
- 担当者は4名に対してキャンセル受付メールを送信していたが、そのうちの１名（Aさん）へのBCC欄に前回イベントの落選者31名のアドレスを入れて送信したため、落選者にAさんの氏名が漏えいした。下書きフォルダに保存されていた過去のメールを誤って使用したため、BCC欄に落選者のアドレスが入ったと考えられる。また、送信時のダブルチェックを実施していなかった。
- 氏名が漏えいしたAさんと誤送信した31名に対して、メールの削除依頼とお詫びを電話またはメールで連絡した。
- 再発防止策として、メールに限らず、不要な個人情報の削除･廃棄を徹底することを求めた。



履行中に遵守すべき事項（５／16）

特(P.17)

（５）情報の持ち出し

重要情報は履行場所から持ち出してはいけません。ただし、区が必要と認めた場合はこの限りではありません。また、持ち出す場合は、以下の事項を守る必要があります。

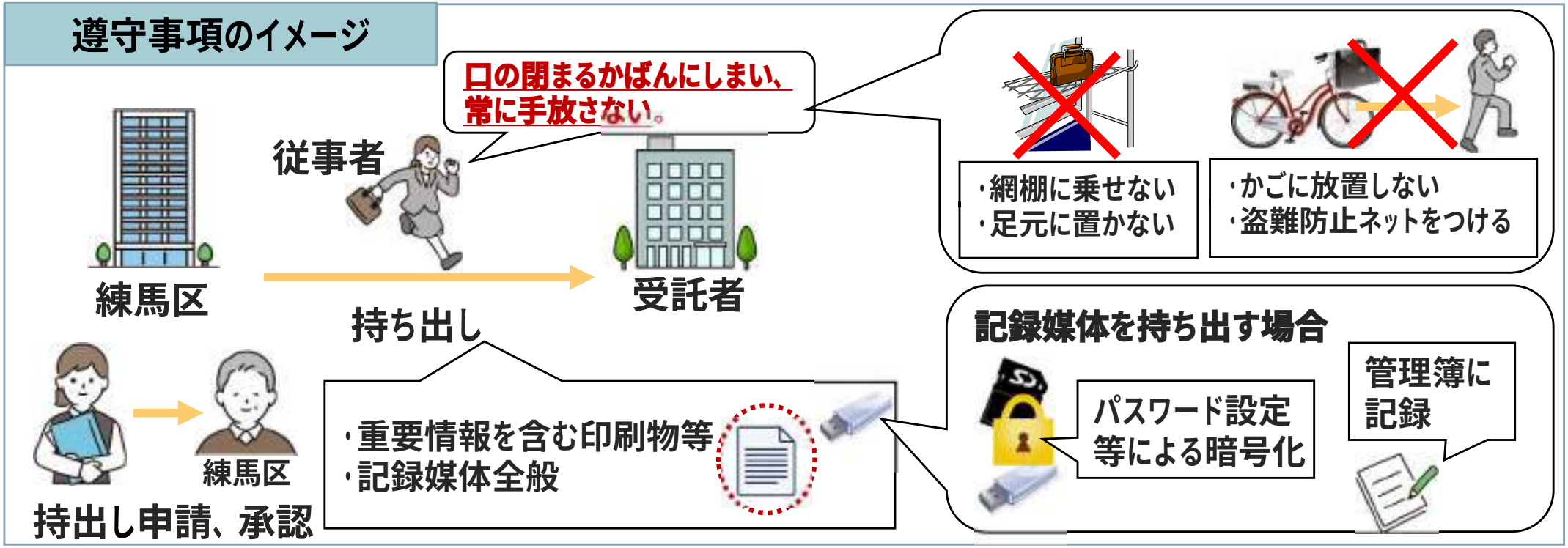
【持ち出し時の遵守事項】

１）受託業務で使用する記録媒体（携帯電話･スマートフォンを含む）、パソコン、印刷物等を持ち運びする時は、**盗難や紛失に十分注意する**。

２）記録媒体は**パスワードを設定する等により、データの暗号化**を行う。

３）情報の格納の有無に係わらず、**記録媒体の持ち出しは、記録を管理簿により管理**する。

遵守事項のイメージ



履行中に遵守すべき事項（５／16）

持ち出し記録の管理方法（例）

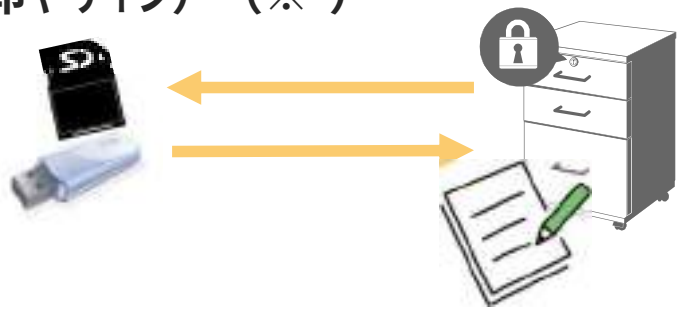
記録媒体の持ち出しは、**「承認～目的の作業が終了し保管場所に戻すまで」を管理簿に記録**し、確実な管理を行う必要があります。

管理簿に記録･管理する項目

記録媒体別に以下を記録･管理します。

ロ 記録簿の項目名

- 利用日
- 利用者
- 利用目的
- 記録媒体への格納情報（情報の内容／重要情報の有無／個人の特定（※1））
- 持ち出し･送付等の種別（持出し先･送付先／送付方法）
- 練馬区（または区から承認権限を与えられた者）の承認（印やサイン）（※2）
- 受領確認日（送付先での受領日）
- 返却確認日（持ち出しの場合）
- データ消去日
- 利用終了日（保管場所への返却日）
- 返却確認（印やサイン）



（※1）紛失等が発生した場合に、誰のどのような情報なのか特定できる情報

（※2）持ち出す機会が多く、都度区の承認を受けることが難しい場合は、予め区と持ち出し時の対応について協議してください

上記の記録媒体別の持ち出し記録とは別に、**記録媒体の管理も必要**です。
項目として、*登録番号*/媒体種類/利用目的/個人情報取扱い有無/所管部署/利用開始日/保管場所/利用終了日/終了方法（廃棄等）/管理者承認等を登録、管理するようにします。

履行中に遵守すべき事項（６／16）

特(P.19)

（６）情報の保管

【保管時の遵守事項】

１）重要情報を含む印刷物･文書や、情報の格納の有無に係わらず、受託業務で使用する記録媒体（携帯電話･スマートフォンを含む）を保管する際は、施錠できるキャビネット等に保管する。

２）情報を格納した記録媒体を保管する際は、適切なアクセス管理を行う。

３）記録媒体において、不要になったデータは直ちに消去し、必ず保管場所に戻す。

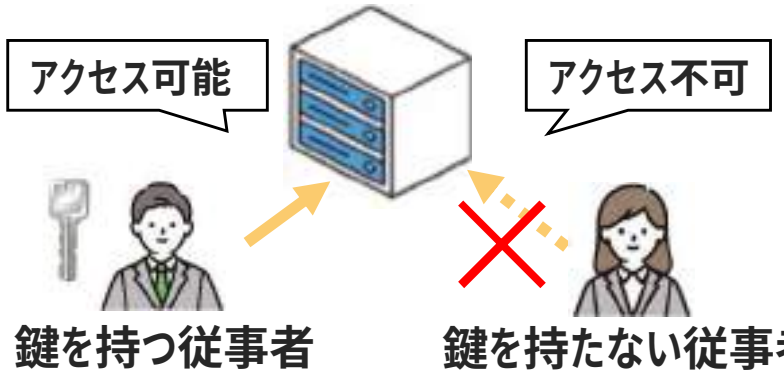
４）重要情報を、受託業務の履行以外の目的のために複写または複製をしない。

５）書類の受け渡しは直接手渡しで行い、決められた場所で管理し、誤廃棄や、持ち出した際の強風等による紛失に注意する。

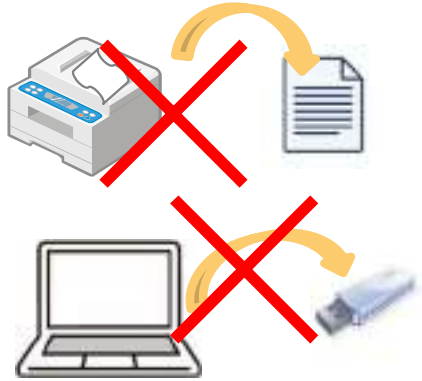
遵守事項のイメージ

● 印刷物･文書や記録媒体は施錠管理する

● 記録媒体で保管する際はアクセス管理を行う



● 履行目的以外の複写や複製は禁止

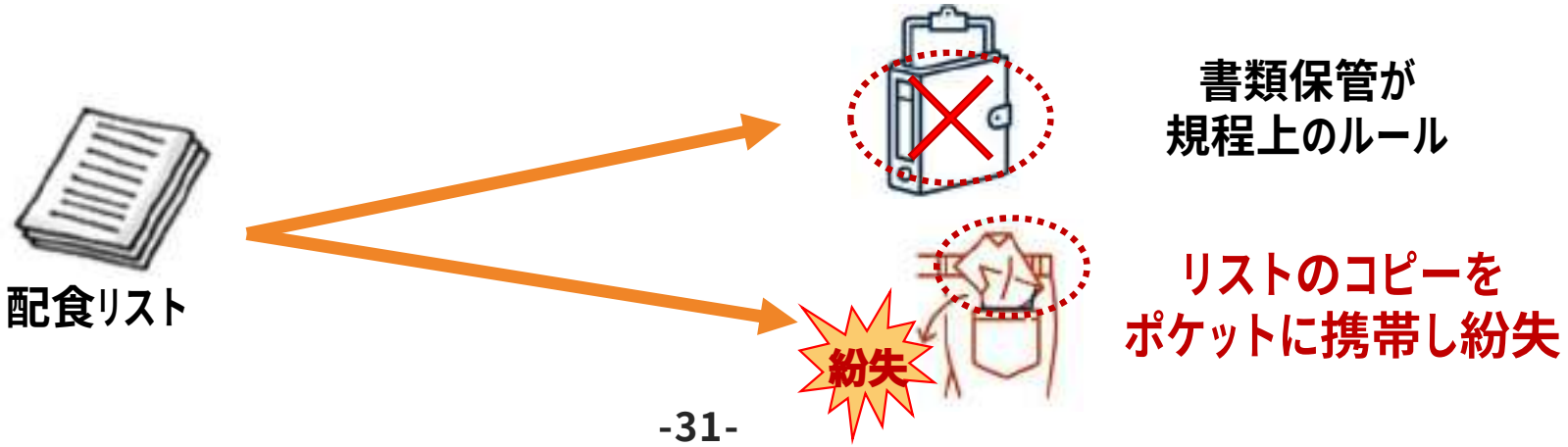


例えば、こんな事故が起きています。

【東村山市】受託者における個人情報の紛失について（令和７年７月）

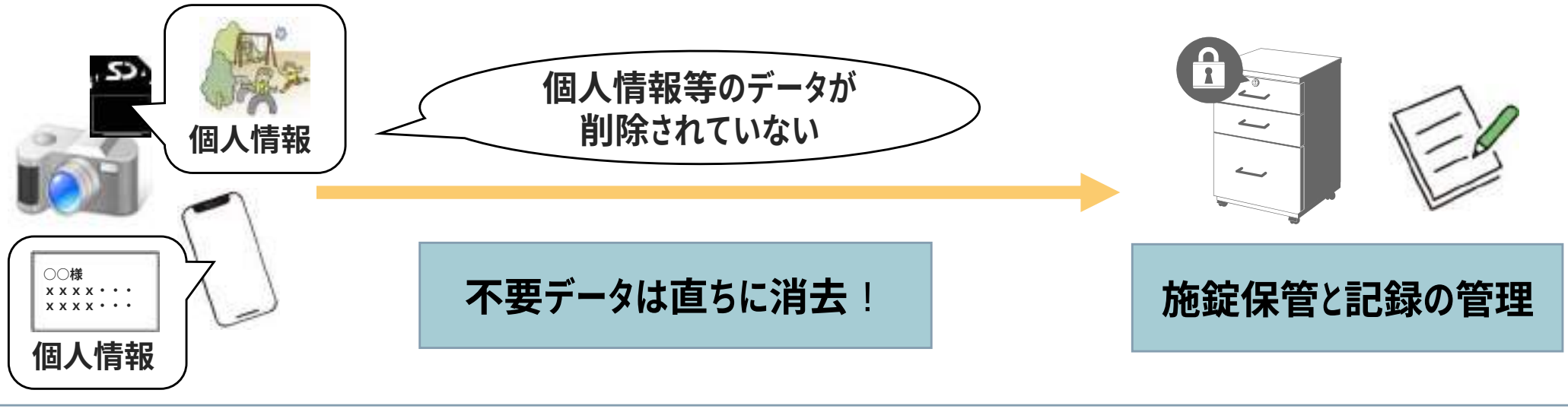
- 「高齢者配食サービス」事業の委託事業者の配送担当者が、当日の配送先である21名分の住所、氏名、電話番号を記載したA4用紙１枚を紛失した。
- 発生原因は、本来は書類として保管するはずのリストのコピーを自身のポケットに携帯し、そのコピーを紛失したことによるもの。
- 対象者に対し、当該事業者から経緯の説明と謝罪を行った。また、市もあらためて経緯の説明と謝罪を行った。
- 再発防止策として、今後、当該事業者に対して、個人情報の取扱いに関する再点検の実施、業務遂行における当日書類の受け渡し時のダブルチェック、関係者への教育指導を徹底した。また、本事業を受託する他の事業者に対しても、今般の情報共有を行うとともに、個人情報の適切な管理について、改めて注意喚起を行った。

（出典：https ://www.city.higashimurayama.tokyo.jp/kenko/korei/korei/files/250718haisyoku.pdf）



情報セキュリティ監査では、ここを指摘しました！

デジタルカメラや携帯電話の個人情報を含むデータを削除していない事業者がいました。



利用後は、<u>不要なデータの削除</u>が必要です。

デジタルカメラや携帯電話を利用した後は、必要に応じて中のデータを決められた場所に保存し、削除することが必要です。

履行中に遵守すべき事項（７／16）

特(P.20)

（７）情報の廃棄

【廃棄時の遵守事項】

１）重要情報を含む印刷物･文書を、裏紙として再利用しない。

２）重要情報を含む印刷物･文書や、情報の格納の有無に係わらず、受託業務で使用した記録媒体（携帯電話･スマートフォンを含む）を廃棄する場合は、データを復元できないよう物理的な破壊または漏えいを来さない方法での消去を行う。

３）記録媒体を廃棄する場合は、その記録を管理簿により管理する。

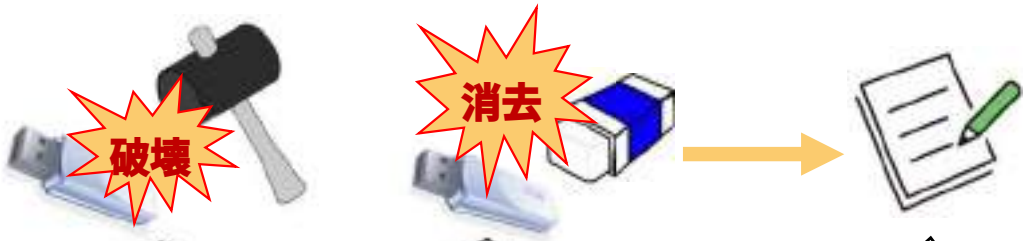
遵守事項のイメージ

- 重要情報を含む印刷物や文書を処分

シュレッダーや溶解処理を用いて復元できないように

ゴミ箱にそのまま捨ててはいけません！

- 記録媒体（携帯電話･スマートフォンを含む）等は、物理的な破壊または漏えいを来さない方法でのデータ消去を行い、管理簿に記録



USBメモリは基盤部分を破壊するか専用ツールでデータを消去する

管理簿に記録

例えば、こんな事故が起きています

【横浜市】小学校防犯カメラの映像含むHDDレコーダーがオークションに（令和4年5月）

- 横浜市内の小学校で利用された屋外防犯カメラと録画用HDDレコーダーが、規定を守らずデータを消去することなく、インターネットオークションで売買されていたことがわかった。
- 同市によれば、2021年10月に委託先事業者が屋外防犯カメラ2台とHDDレコーダーの取替え工事を行ったが、取り外したカメラとレコーダーの処分の依頼先従業員がインターネットオークションを通じて売却していた。
- 防犯カメラでは、小学校の昇降口や裏手の校門を撮影しており、不特定多数の児童、学校職員などが映っていた。
- レコーダーの落札者から同市教育委員会に、学校を撮影したと思われる映像が残っているとの問合せがあり判明した。委託先が落札者と連絡を取りレコーダーを回収した。

（出典：https ://www.security-next.com/136524）

履行中に遵守すべき事項（８／16）

特(P.21)

（８）情報システムでの作業

情報システムで作業する場合は、以下の事項を遵守する必要があります。

【情報システムで作業する場合の遵守事項①】　（受託者が情報システムを用意する場合）

１）IDとパスワード等による認証を実施※1する。情報漏えい等のリスクがあるため、必要な場合を除きIDとパスワードは共用しない。

２）インターネットに接続された環境で重要情報を取り扱う場合は、標的型攻撃等の不正アクセスによる重要情報の漏えい等が生じないよう適切な措置を講じる。

３）ウィルス対策ソフトウェアの導入およびウィルスパターンファイルの最新化を行う。

４）OS、ミドルウェア等に、定期的に修正プログラムを適用する。

５）許可のない記録媒体の接続やソフトウェアのインストールがされないよう、適切な措置を講じる※2。

６）離席時にスクリーンセーバ等により自動でロックする設定を行う。

※1　IDとパスワードは、他人に知られないように管理してください。また、パスワードは、原則として大小英字、数字、記号のうち３種類以上を組み合わせた10文字以上（最低８文字）としましょう。

※2　記録媒体やソフトウェアのインストールは可能な限り技術的な対策（制限ユーザー等）で制限してください。費用対効果等の面から難しい場合は、運用による対策が徹底されるよう、適切に管理してください。

履行中に遵守すべき事項（８／16）

特(P.21)

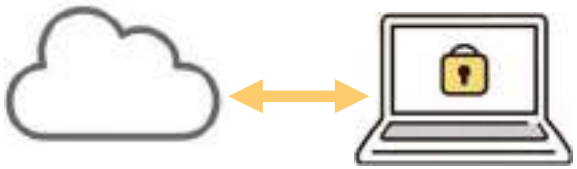
（８）情報システムでの作業（つづき）

【情報システムで作業する場合の遵守事項②】（区および受託者のシステムの共通事項）

１）複数の情報システムや記録媒体を使う場合、互いに異なるパスワードを設定する。
２）インターネットに接続された環境で重要情報を取り扱う場合は、パスワードを設定する等によりデータを暗号化する。
３）従事者の私物等、許可されていない情報システムおよび記録媒体は使用しない。
４）受託業務で使用する記録媒体を情報システムに接続する場合は、ウィルスチェックを行う。
５）情報を処理する情報システムにはWinny、Share等のファイル交換ソフトをインストールしない。また、許可されていないソフトウェアをインストールしない。
６）区の情報システムの利用や運用保守作業等を行う時は、区の示す手順（利用マニュアル、管理マニュアル、運用設計、基本設計等）を遵守する。

遵守事項のイメージ

● インターネットに接続された環境で重要情報を取り扱う場合



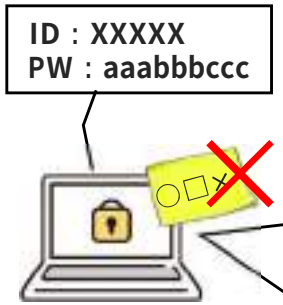
- パスワードを設定する等により暗号化
- 不要になったファイル等は、速やかに削除
- ファイアウォール等で、登録の無い通信先との通信を遮断

履行中に遵守すべき事項（８／16）

特(P.21)

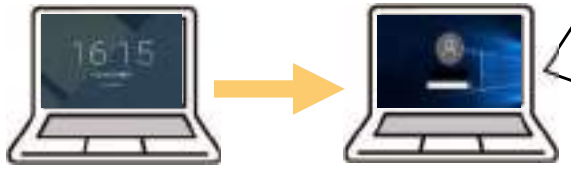
遵守事項のイメージ（つづき）

● IDとパスワードの設定に関する留意点



- IDやパスワードは、他人に知られないように管理
- パスワード は、原則として大小英字、数字、記号のうち３種類以上を組み合わせた10文字以上（最低８文字）にする
- 複数のシステムを使用する場合、異なるパスワードを設定

● 受託業務で使用する情報システムの設定



スクリーンセーバ　　パスワードロック

- スクリーンセーバ等により自動でロックする設定
- 許可のない記録媒体の接続やソフトウェアのインストールを制限

● 使用してはいけないパソコン等

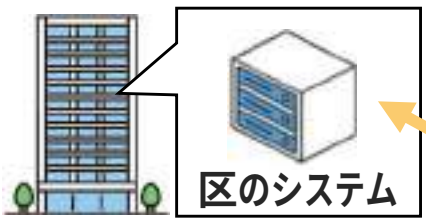
私物のパソコンや記録媒体等

Winny、Share等、無許可のソフトがインストールされた機器

● 情報システムに行うウィルス対策

- ウィルス対策ソフトの導入
- ウィルスパターンファイルの更新
- OS等の修正プログラムの適用
- 記録媒体を情報システム機器に接続する際のウィルスチェック

● 区の情報システムの利用や運用保守作業等を行う時



従事者

手順を遵守

運用保守作業者

運用設計、基本設計、その他実施手順

履行中に遵守すべき事項（９／16）

特(P.22)

（９）クラウドサービスの利用

重要情報の取扱いにクラウドサービスを利用する場合は、以下の点に留意する必要があります。

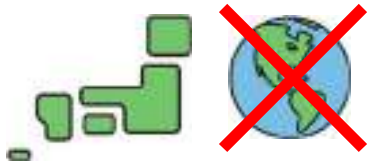
【クラウドサービス利用時の遵守事項】

１）**日本の法令の範囲内で運用**できるサービスであること。

２）サービス提供するリージョン（国・地域）を国内に指定でき、**データが海外に保存されない**こと。

３）次の事項を契約またはサービスレベル契約（SLA）に定められること。

- ✓ クラウドサービスの**終了または変更時における事前通知などの取り決めや、情報資産の移行方法**
- ✓ **情報セキュリティ対策の履行が不十分な場合の対処**方法（改善、追完、損害賠償等）
- ✓ クラウドサービス提供者が、**情報資産へ目的外のアクセスや利用を行わない**こと
- ✓ **情報セキュリティインシデント（情報セキュリティ事故およびその兆候）への対処**方法



４）情報セキュリティ対策の実施内容および管理体制について、公開資料や監査報告書、各種の認定・認証制度の適用状況から、総合的・客観的に評価し、判断可能であること。

５）次の事項を技術的に満たすこと。

- ✓ **アクセス制御**ができる
- ✓ クラウドサービス内および通信経路全般に**暗号化処理**が行われる
- ✓ **各種ログの取得**機能を実装している
- ✓ クラウドサービスの**利用終了時に、全ての情報が漏えいしない方法で確実に削除**される

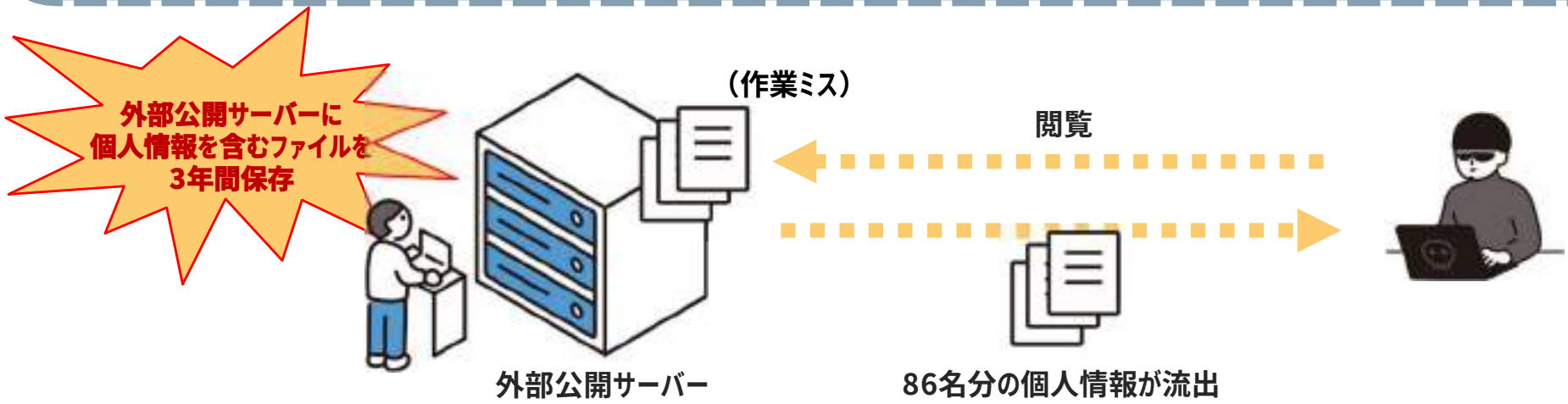
※　上記事項を満たすとしても、従事者は**個人で契約しているクラウドサービスに、受託業務に係る情報を保存してはいけません。**

例えば、こんな事故が起きています

【茨城県】外部公開サーバーに登録された個人情報の漏えい （令和７年５月）

- 県民などから寄せられた意見や提案を記録するシステムにおいて、個人情報が含まれるファイルが外部公開用サーバーに保存され、インターネット上で閲覧可能な状態になっていた。流出が確認されたのは、2022年7月に県へ相談などを行った86名分の個人情報で、最大で264回の閲覧があった形跡がある。
- システムの保守業務を委託している事業者がシステムの出力テストを実施した際に、個人情報が含まれるファイルを誤って外部公開用サーバーに残したことが原因とされている。その後、約3年間にわたり、ファイルは削除されることなく、非公開のURLを知っていればアクセス可能な状態が続いていた。
- 再発防止策として、外部公開用サーバーに個人情報を含むファイルが存在しないことの確認を業者に徹底し、２ケ月に１回の定期保守の際、確認結果の報告を義務づける運用とした。

（出典：https://www.pref.ibaraki.jp/somu/hodo/hodo/pressrelease/hodohappyoushiryou/2203/documents/250513hodo.pdf）



履行中に遵守すべき事項（10／16）

（10）携帯電話･スマートフォンの使用

受託業務で携帯電話やスマートフォンを使用する場合は、以下の点に留意する必要があります。

【携帯電話･スマートフォン使用時の遵守事項】

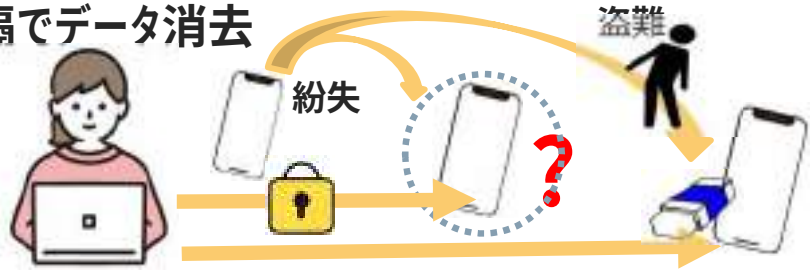
1）持ち出す場合は、肌身離さず持ち歩くなど、紛失や盗難に十分注意し、持ち出しの記録を管理簿により管理する。
2）使用後に不要になったデータを直ちに消去する。
3）パスワード等のロックを設定し、紛失や盗難時に備えて、遠隔でのロックや遠隔データ消去のサービスを利用する（推奨）。
4）従事者の私物等、許可されていない携帯電話やスマートフォンは使用しない。
5）LINE等、SNSの個人アカウントで、受託業務で取り扱う情報をやり取りしない。

遵守事項のイメージ

- パスワード等のロックを設定する

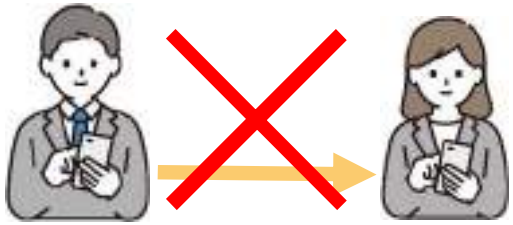
- 紛失や盗難時に利用されないように、遠隔からコントロールを可能にする

･遠隔でロック
･遠隔でデータ消去



- 受託業務で取り扱う情報をSNS（LINE等）でやり取りしない

LINEで情報を送信



例えば、こんな事故が起きています。

【原子力規制庁】私用で訪問した中国で業務用携帯電話を紛失（令和７年11月）

- 原子力規制庁の職員が私用で訪問した中国で業務用のスマートフォンを紛失していたことが分かった。スマートフォンには機密性が高いため公表していない核セキュリティ担当部署の職員名や連絡先が登録されていた。スマートフォンは発見できず、原子力規制庁は「情報漏洩の可能性が否定できない」として、国の個人情報保護委員会に報告した。
- 上海の空港で、保安検査を受けるために手荷物を出した際に紛失したとみられる。3日後に紛失に気づき、空港などに問い合わせたが見つからなかった。電波が届かず遠隔操作でのロックやデータ消去も難しい。
- 原子力規制庁は、庁内への注意喚起や再発防止に努めるとした上で「海外渡航時などのスマホ携行に関するルールを整理したい」とした。

（出典：https://www.nikkei.com/article/DGXZQOUA07BM10X00C26A1000000/?msockid=0f3438c2a44c66203e172db2a56e6790）

履行中に遵守すべき事項（11／16）

特(P.23)

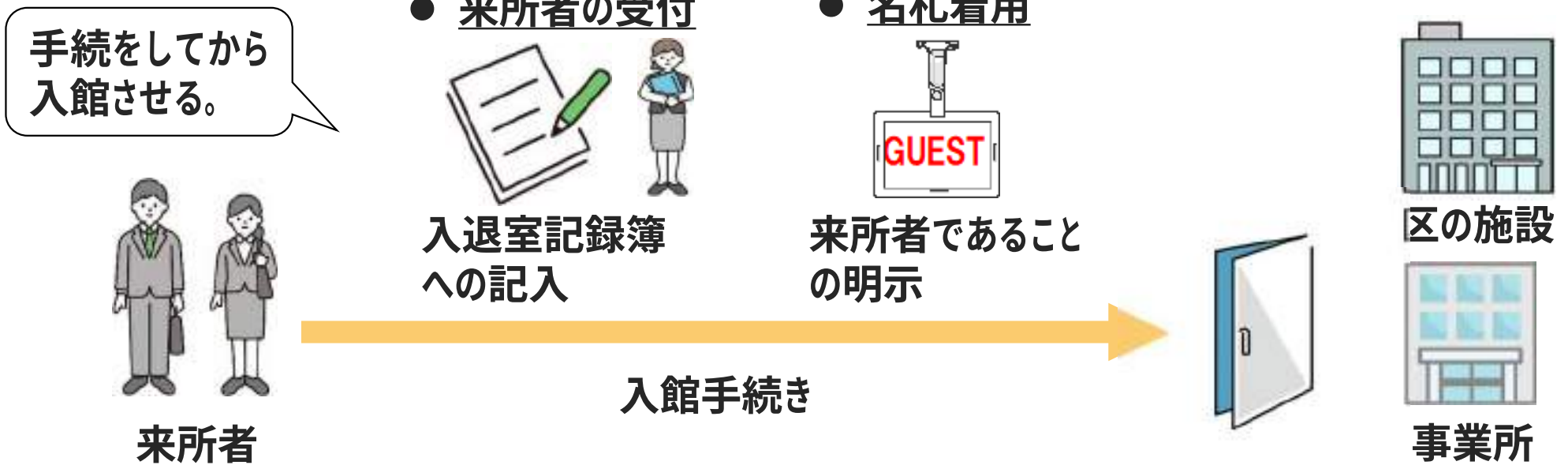
（11）施設の入退室管理

許可された者以外の入退室を防ぐとともに、情報が脅威にさらされた場合、原因を迅速に特定できるようにするため、以下の点に留意する必要があります。

【施設への入退室に関する遵守事項】

施設や事業所など、情報を取り扱う場所においては、来所者の受付や名札着用など、入退室管理を行う。

遵守事項のイメージ



例えば、こんな事故が起きています

【柏崎刈羽原発】原発の心臓部に不正入室　ID「不一致」警報でも入室許可、社員が独断で認証情報変更も（令和２年２月）

- 東京電力柏崎刈羽原発（新潟県）で、令和２年９月に社員が同僚のIDカードを無断使用して中央制御室に入っていたことが判明した。
- 入室の際に、２ヶ所の出入り口でIDと本人確認の疑念や認証情報が「不一致」という警報が出たにもかかわらず、警備員や警備担当社員が入室を許可していた。
- 警備担当社員は、入域を認めた上、認証情報を不正入室した社員のものに独断で変更した。翌日、本来の持ち主が入室できず、IDの不正利用が発覚した。
- 中央制御室は原子炉を操作する設備で、危機管理上入退室が厳しく制限されているが、ずさんな危機管理体制が明らかになった。

（出典：https ://www.tepco.co.jp/niigata_hq/kk-np/kaikaku/id-card.html ）

履行中に遵守すべき事項（12／16）

（12）ソーシャルメディアの利用について

ソーシャルメディアで発信した情報は、瞬時に不特定多数の人々に公開されます。投稿内容によっては、区、所属する組織および自身の信用失墜につながるため、以下の点に留意する必要があります。

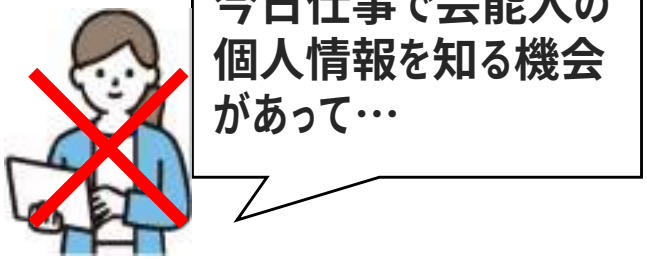
【ソーシャルメディア利用時の遵守事項】

1）ソーシャルメディアには、**受託業務で取り扱う情報を書き込まない。**また、**LINEやInstagram等のSNSで当該情報をやり取りしない**。

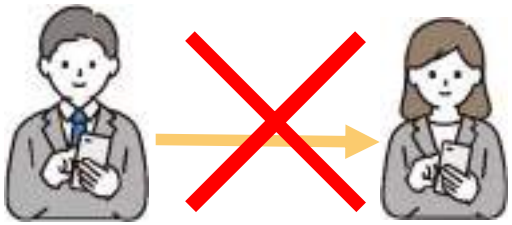
2）ソーシャルメディアにより情報を発信する必要がある場合、**インターネット上に公開して良い情報かそうでないかを正しく判断する**。

遵守事項のイメージ

- 当該契約で取り扱う情報は書き込まない



- 情報をSNS（LINE等）でやり取りしない（※再掲）



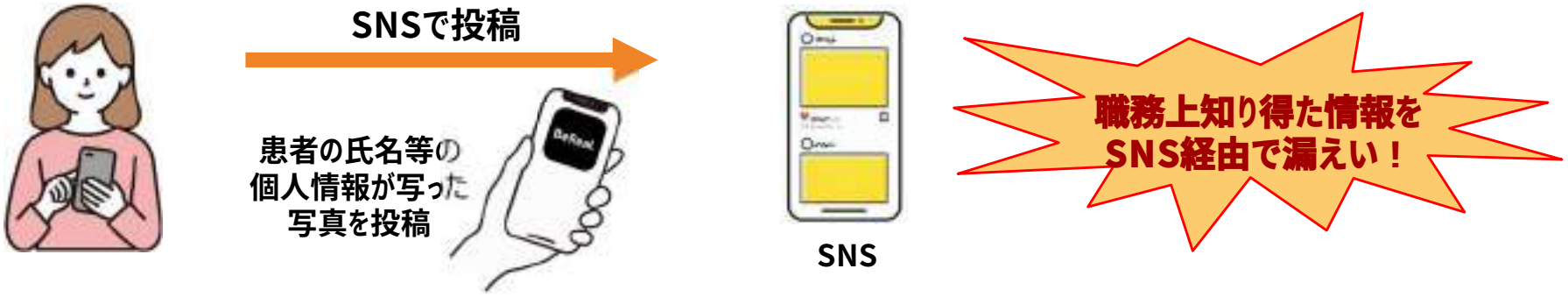
- 公開の範囲を意識して利用する

例えば、こんな事故が起きています。

【岩見沢市立総合病院】委託職員が病院の受付状況をSNSに投稿　（令和７年11月）

- 岩見沢市立総合病院で個人情報がSNS上に投稿されている事態が判明した。外来受付業務を委託している業者の職員が、患者20名分の個人情報を含むモニター画面を私物のスマートフォンで撮影していた。
- 投稿された画像には、同日来院した患者20名の氏名、患者番号、性別、年齢、主治医名が映っており、個人情報保護法で定める「要配慮個人情報」に該当する内容だった。投稿は閲覧制限がかかった状態だったが、誰でも見られる可能性があったとされている。病院によると、投稿は市民からの通報で発覚。病院の調べでは、情報の二次流出は確認されなかったとされている。
- 対象となった患者20名全員に対し、病院職員が直接謝罪。再発防止策として、当該職員は即日業務から外し、委託事業者に対しては業務中のスマートフォン持ち込み・使用を原則禁止とするルールを導入している。また、委託業者全職員に臨時の情報管理研修を実施し、今後も定期的に開催する方針とした。

（出典：https ://www.iwamizawa-hospital.jp/news/details/post_188.html）



履行中に遵守すべき事項（13／16）

（13）Web会議の利用について

受託業務でWeb会議を利用する場合は、以下の点に留意する必要があります。

【Web会議利用時の遵守事項】

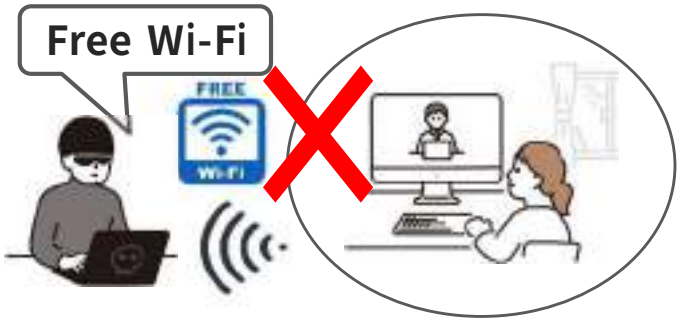
1）機密性の高い会議への利用は、**管理責任者が必要性が高いと判断した場合**に限る。
2）**重要情報が映り込まない、周囲の会話や電話等の音声が入らない場所**で利用する。
3）会議のURL、ID、パスコードなどは、**参加者のみに知らせ、使い回しをしない**。
4）全員の参加を確認後、会議をロックするなど、**第三者が参加できないようにする**。
5）会議資料は原則メール等で参加者へ送付し、重要情報を含む資料は**画面共有しない**。
また、重要情報を含むファイルのアップロードはしない。
6）会議の通信では、傍受されるリスクのある**フリーWi-Fi等は利用しない**。

遵守事項のイメージ

- 重要情報の画面共有はしない

- 会話や電話等の音声が入らない場所で利用する

- 傍受されるリスクのある通信環境は利用しない



履行中に遵守すべき事項（14／16）

（14）テレワークについて

受託業務をテレワークで行う場合は、以下の点に留意する必要があります。

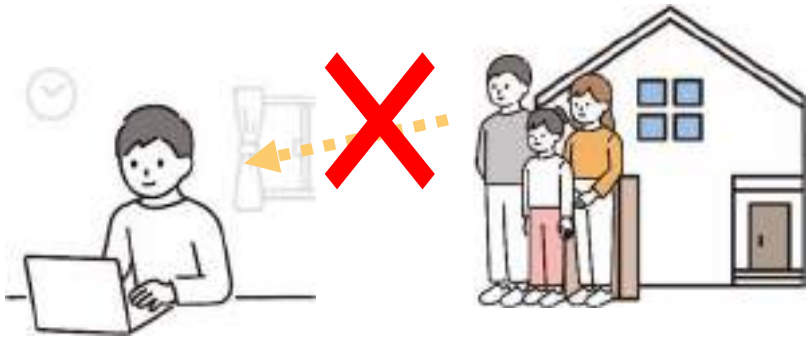
【テレワーク実施時の遵守事項】

１）関係者以外（家族を含む）に見られない場所で作業する。

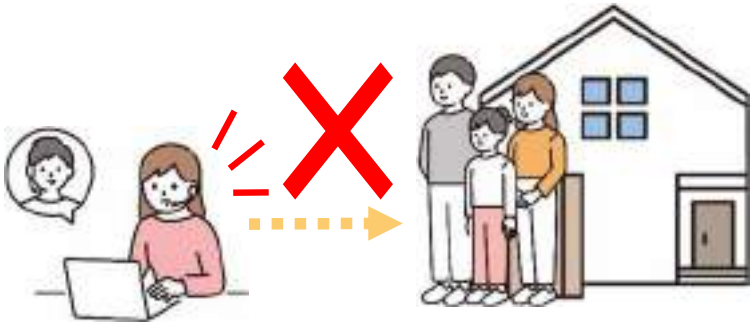
２）関係者以外（家族を含む）がいる場所で重要情報を含む会話をしない。

遵守事項のイメージ

- 関係者以外に見られない場所で作業する



- 関係者以外がいる場所で重要情報を含む会話をしない



履行中に遵守すべき事項（15／16）

（15）なりすまし等の防止

情報窃取の手段として、なりすましや盗み聞き等の「ソーシャルエンジニアリング」があります。

【ソーシャルエンジニアリング防止のための遵守事項】

１）電話をかけた時に留守番電話であった場合、<u>個人情報を含む内容を録音しない</u>。

２）電話での問い合わせでは、こちらからかけ直すなどして、<u>本人以外の人に情報を伝えない</u>。

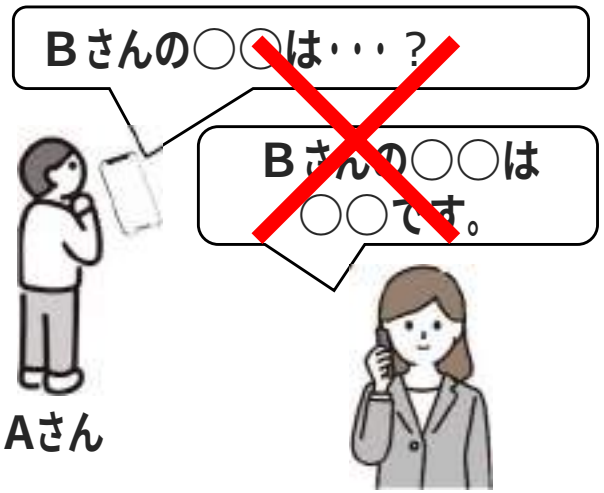
３）第三者がいる場所で、<u>個人情報を含んだ会話をしない</u>。

遵守事項のイメージ

● <u>本人以外に本人の情報を伝えない</u>

（電話をかけた場合）

（電話を受けた場合）



● <u>第三者がいる場所で、個人情報を含んだ会話をしない</u>

履行中に遵守すべき事項（16／16）

（16）事故等発生時の対応

【情報セキュリティ事故等が生じた場合の遵守事項】

１）直ちに応急処置を行うとともに、管理責任者に報告する（管理責任者は直ちに区に報告する）。

２）事故等の原因を特定するため、証拠を保全しつつ事故および対応の過程を記録する。

３）原因を分析し、再発防止策まで含む報告書を作成する。

遵守事項のイメージ

直ちに区に事故等の第一報を報告

- 事故等を発見した時は・・・

例：ウィルスに感染！

応急処置

LANケーブルを抜く

管理責任者に直ちに報告

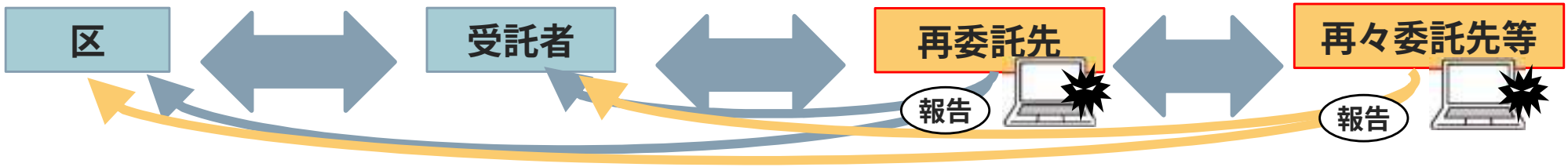
従事者

管理責任者

証拠を保全し、事故等の記録をとる

原因分析、再発防止策の検討

- 再委託先・再々委託先等で事故等が起きた場合、区および委託先に報告



第４章　契約終了時に実施すべき事項

対象：受託者

本章は、受託者が契約終了時に実施すべき事項を記載しています。

契約終了時に実施すべき事項

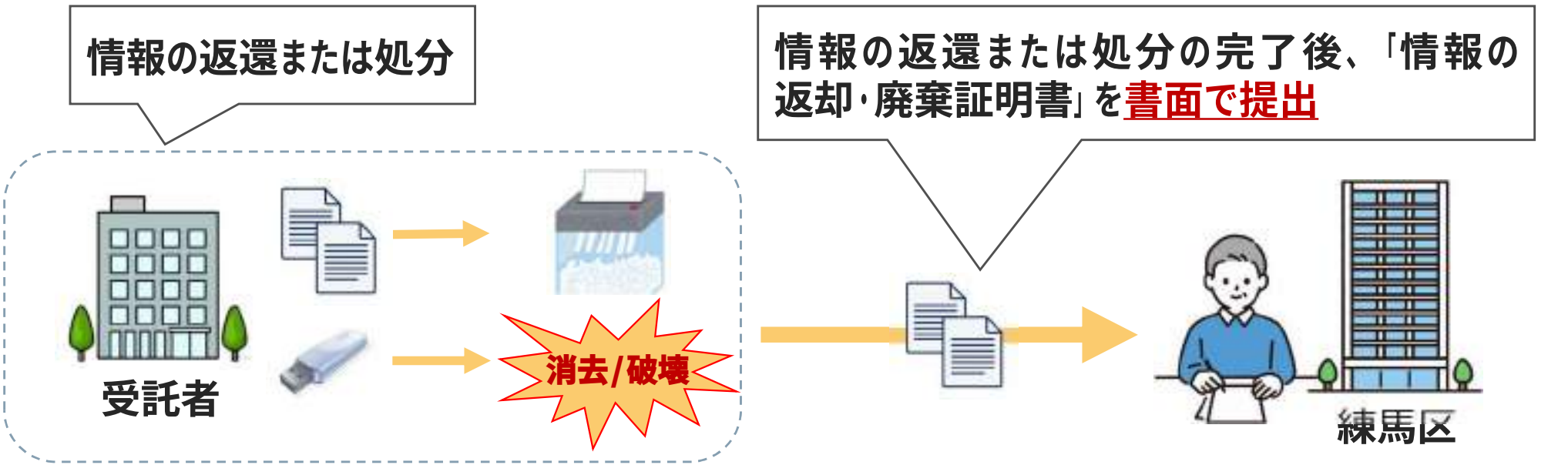
特(P.26)

ａ．情報の返還･処分

あらかじめ、業務の終了後に情報を返還するか処分するかを取り決める必要があります。
受託者は契約終了の際に、情報について区に返還するか漏えいを来さない方法で確実に処分して、その結果を区に書面で報告する必要があります。
※　契約期間中に、外部委託により処分する場合も含まれます。

しなければならないこと

※　書面の参考様式は、区から提示します。

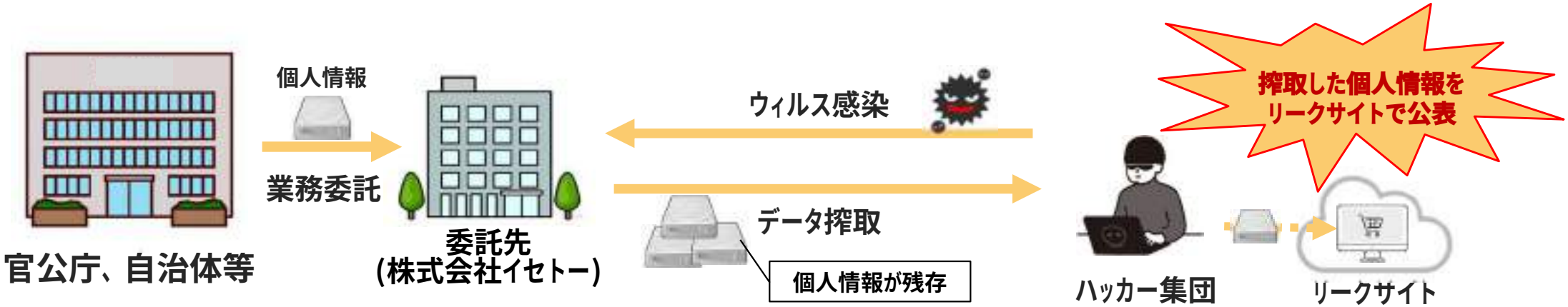


例えば、こんな事故が起きています

【徳島県等】契約終了後にデータを削除せず、サイバー攻撃被害で情報漏えい（令和６年５月）

- 株式会社イセトーは、VPN回線からの不正アクセスにより、自社の複数サーバやPCがランサムウェア被害に遭い、官公庁や自治体等から預かっていた各種個人情報が漏えいし、第三者によって一部情報がリークサイトで公表されたことを発表した。
- 徳島県は20万人以上、和歌山市は15万人、豊田市は14万人等、20以上の自治体等で被害が報告されている。
- 同社は、**個人情報を含むデータについて契約終了時点で消去したと報告していたが、実際には消去していなかった**。また、**作業効率を図るため、本来個人情報を取り扱いできないネットワークやPCに個人情報を保管していた**ことが判明した。
- 同社は、複数の自治体等から入札指名停止となり、損害賠償も検討されている。また、ISO27001認証およびISO27017認証、プライバシーマーク付与が一時停止となっている。現在は、ISO認証、プライバシーマーク付与共に一時停止が解除されている。

出典： https://www.yomiuri.co.jp/national/20240801-OYT1T50161/
https://www.iseto.co.jp/news/news_202503-1.html



第５章　再委託について

対象：受託者

本章は、受託者が再委託や再々委託等をする場合に実施すべき事項を記載しています。

再委託について

ａ．再委託の制限

受託業務の再委託や再々委託等（※）（以下、「再委託等」という。）について、次の事項を遵守する必要があります。

【再委託等に関する遵守事項】

（１）やむを得ず、再委託等（再々委託等の場合は、個人情報を取り扱う場合のみ。以下同じ。）を行う場合は、区から承認を得る（承認申請書を提出する）。

業務内容に特定個人情報（マイナンバー）を含む場合、委託事業者が区の許諾を得ずに再委託等をしていることが判明した場合は、番号法に抵触するため、個人情報保護委員会への報告対象となります！

（２）個人情報を取り扱う再委託等の場合は、契約締結前に当該契約の受託予定者において、特記事項等に規定する安全管理措置が講じられることをあらかじめ確認し、指定する書面により区に提出する（（１）の書類と併せて提出する）。

★作成するのは、再委託等の受託予定者。提出するのは受託者。

（３）再委託等を行う場合には、特記事項と同等以上の規定を設けて契約する。

（４）再委託等を行う場合、当該契約の受託者（以下「再委託先等」という。）に、受託業務における一切の義務を遵守させるとともに、その履行状況を監督する。

（※）再々委託等：再委託先がさらに第三者に再委託する場合（それ以降の委託を含む）

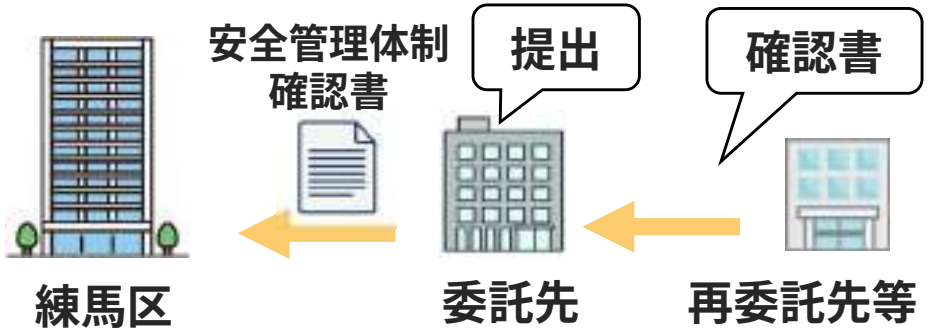
再委託について

ａ．再委託の制限（つづき）

遵守事項のイメージ

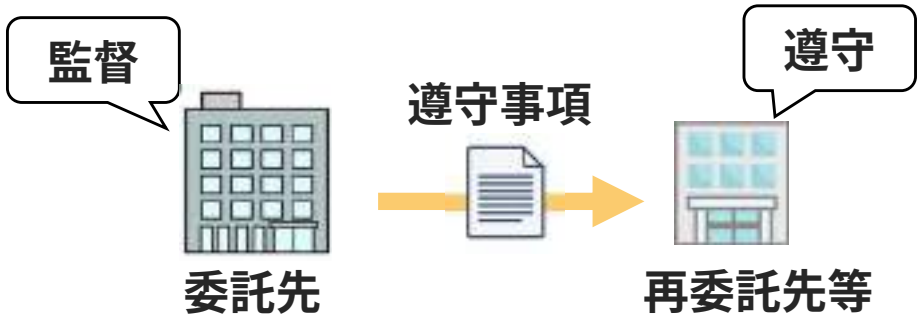
- 区から承認を得る

- 個人情報を扱う場合は、「安全管理体制確認書」を提出させる



- 特記事項と同等以上の規定とする

- 受託者における一切の義務を遵守させ、履行状況を監督する

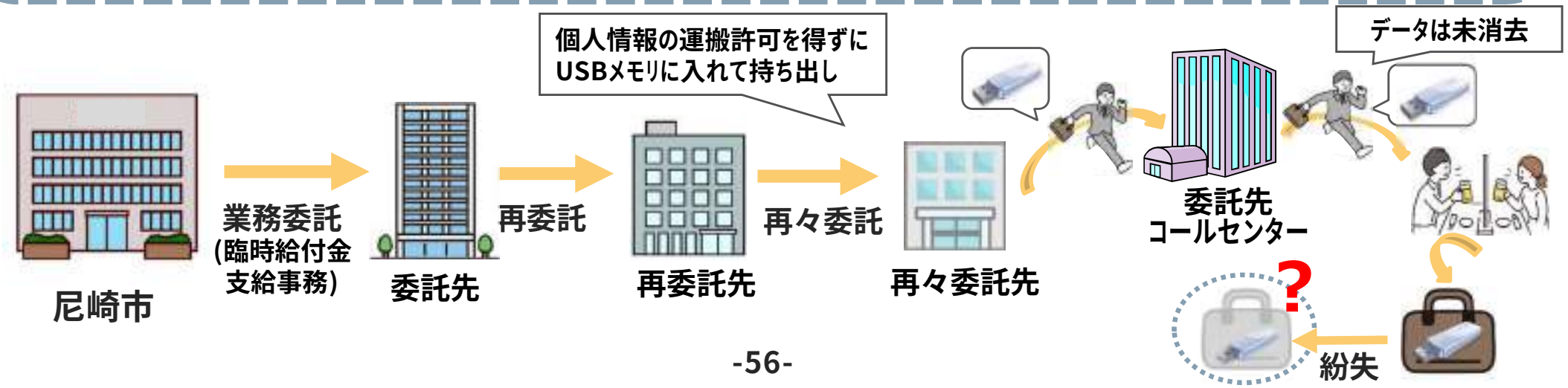


例えば、こんな事故が起きています

【尼崎市】個人情報を含むUSBメモリの紛失（令和４年６月）

- 尼崎市は、同市全住民の**個人情報を含むUSBメモリが所在不明**となっていることを明らかにした。
- 臨時給付金支給事務の**再々委託先従業員**が、全市民46万人の住民基本情報を含む個人情報約100万件が入ったUSBメモリ2つを、市の庁舎から事業者のコールセンターへ持ち出し、データを移管した後、**データを消去せずにコールセンターから持ち出し、飲酒を伴う食事の後、泥酔してカバンごと紛失**した。当該USBメモリにはパスワードが付与され、内容は暗号化されていた。当該USBは事故発生3日後に発見された。
- 受託者は、委託者の事業所外でのデータ処理の許可を得ていたが、受託者の関係社員個人が記録媒体で**個人情報を運搬する具体的手法については、同市から許可を得ていなかった**。また、市は受託者に対し、持ち出す際に許可を得るべき旨を徹底していなかった。
- 加えて、受託者において、データ消去がされていない当該USBメモリを所持している作業者に対し、飲酒を伴う食事への参加を注意しない等、管理監督が適切に行われていなかった。

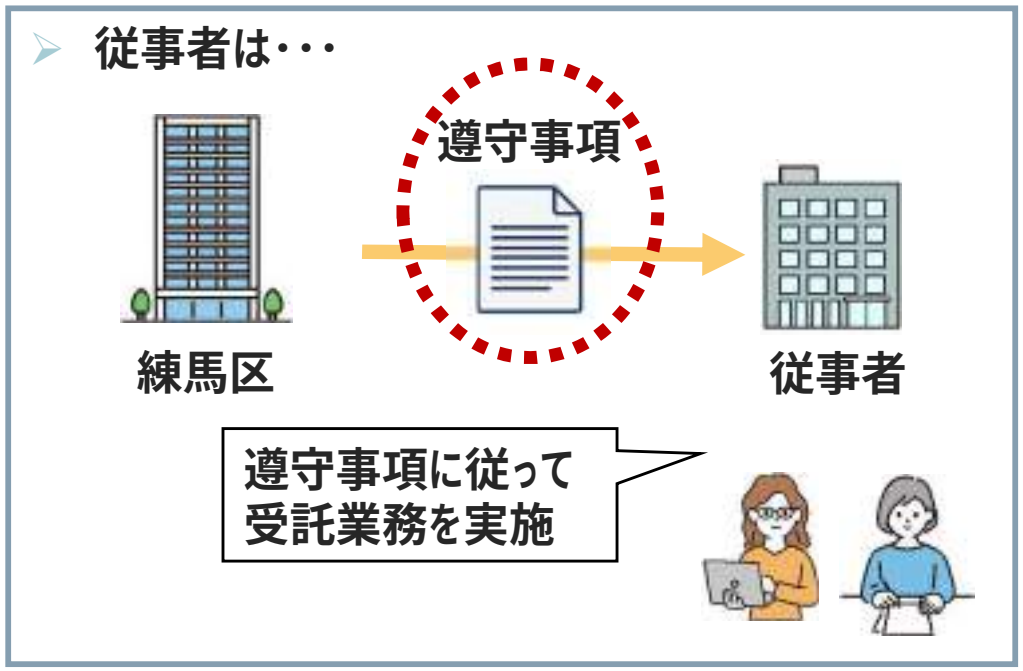
（出典： https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html）



おわりに

特(P.24)

受託者およびその従事者が特記事項の内容を理解し遵守することは、情報セキュリティ事故等を防止することにつながります。
日ごろから、遵守事項や関係法令等に基づいて、情報を適切に取り扱うよう心がけてください。
なお、情報の取扱いに関して、区から受託者へ立入検査や監査を行う場合があります。その際には、ご協力ください。



復習テスト

対象：管理責任者、従事者

受託業務に従事する方が、第３章で学んだことの確認
および教材内容の復習を行うためのテストです。

遵守事項の復習（１）

- 今回の教材で取り上げた遵守事項について、〇か×で解答してください。

	○or×	設問
情報の郵送 (P.21)		重要情報を格納する時は、中身の入れ違いがないか確認し、追跡可能な移送手段を用いる。
情報の送信 (P.24) メールの利用 (P.25、26)		不審なメールを受信した際は、正当性が確認できるまでは添付ファイルを開いてはならないが、メール本文のURLもクリックしてはならない。
		情報をメールやFAXで送信する時は、宛先および添付ファイルを誤らないように十分注意する。
		複数人に一斉にメールを送る際は、メールアドレスを「CC」に設定する。
情報の持ち出し (P.28、29)		USBメモリが入った仕事用のカバンを持ち出す際は、電車の中では安全のため足元に置いておく。
		記録媒体を持ち出す際は、持ち出しの承認から返却までを管理簿に記録する。
		記録媒体を外部に持ち出す際は、個人情報等の重要情報が無い場合は、データにパスワードを設定しなくても良い。
情報の廃棄 (P.33)		受託業務終了後、業務で使用したデータを格納しているUSBメモリやSDカードは物理的な破壊または漏えいを来さない方法でデータを消去する必要がある。

（次ページに続く）

遵守事項の復習（２）

（前ページの続き）

	○or✕	設問
情報システムでの作業 (P.35～37)		複数の情報システムや記録媒体を使う際は、十分に安全な10文字以上のパスワードを設定する。
		受託業務を履行する上で情報システムを用意する際は、ウィルス対策ソフトウェアの導入が必要だが、ウィルスパターンファイルの最新化まで実施する必要がある。
		情報を処理する情報システムには、ファイル交換ソフトをインストールしない。また、許可されていないソフトウェアをインストールしない。
クラウドサービスの利用 (P.38)		クラウドサービスを利用する際は、日本の法令の範囲内で運用できるサービスである必要はない。
ソーシャルメディアの利用 (P.44)		受託業務で取り扱う情報について、InstagramやX等のSNSでやり取りしてはいけないが、LINEで情報を送信することは問題ない。
Web会議の利用 (P.46)		Web会議を行う際は、重要情報が映り込まない、周囲の会話や電話等の音声が入らない場所で利用する。
事故発生時の対応 (P.49)		情報セキュリティ事故等が発生した際は、直ちに応急処置を行うとともに、管理責任者に報告する(管理責任者は直ちに区へ報告する）。
再委託 (P.54,55)		受託業務を再委託する際は、受託事業者と再委託事業者間での契約になるため、区への承認申請は不要である。

解答（１）

- 正解は以下のとおりです。

	○or✕	設問
情報の郵送 (P.21)	○	重要情報を格納する時は、中身の入れ違いがないか確認し、追跡可能な移送手段を用いる。
情報の送信 (P.24) メールの利用 (P.25、26)	○	不審なメールを受信した際は、正当性が確認できるまでは添付ファイルを開いてはならないが、メール本文のURLもクリックしてはならない。
	○	情報をメールやFAXで送信する時は、宛先および添付ファイルを誤らないように十分注意する。
	✕	複数人に一斉にメールを送る際は、メールアドレスを「CC」に設定する。
情報の持ち出し (P.28、29)	✕	USBメモリが入った仕事用のカバンを持ち出す際は、電車の中では安全のため足元に置いておく。
	○	記録媒体を持ち出す際は、持ち出しの承認から返却までを管理簿に記録する。
	✕	記録媒体を外部に持ち出す際は、個人情報等の重要情報が無い場合は、データにパスワードを設定しなくても良い。
情報の廃棄 (P.33)	○	受託業務終了後、業務で使用したデータを格納しているUSBメモリやSDカードは物理的な破壊または漏えいを来さない方法でデータを消去する必要がある。

（次ページに続く）

解答（２）

（前ページの続き）

	○or✕	設問
情報システムでの作業 (P.35～37)	✕	複数の情報システムや記録媒体を使う際は、十分に安全な10文字以上のパスワードを設定する。
	○	受託業務を履行する上で情報システムを用意する際は、ウィルス対策ソフトウェアの導入が必要だが、ウィルスパターンファイルの最新化まで実施する必要がある。
	○	情報を処理する情報システムには、ファイル交換ソフトをインストールしない。また、許可されていないソフトウェアをインストールしない。
クラウドサービスの利用 (P.38)	✕	クラウドサービスを利用する際は、日本の法令の範囲内で運用できるサービスである必要はない。
ソーシャルメディアの利用 (P.44)	✕	受託業務で取り扱う情報について、InstagramやX等のSNSでやり取りしてはいけないが、LINEで情報を送信することは問題ない。
Web会議の利用 (P.46)	○	Web会議を行う際は、重要情報が映り込まない、周囲の会話や電話等の音声が入らない場所で利用する。
事故発生時の対応 (P.49)	○	情報セキュリティ事故等が発生した際は、直ちに応急処置を行うとともに、管理責任者に報告する(管理責任者は直ちに区へ報告する）。
再委託 (P.54,55)	✕	受託業務を再委託する際は、受託事業者と再委託事業者間での契約になるため、区への承認申請は不要である。

［ 参考情報 ］ ランサムウェア攻撃を受けた場合

情報システムで作業している際に以下の事象が確認された場合は、ランサムウェア攻撃(※)を受けている可能性があります。

- ✓ ネットワーク内部の複数のシステムでファイルの拡張子が変わり、開封できなくなった
- ✓ 自組織から窃取されたとみられるファイルを暴露する投稿が行われた
- ✓ 攻撃者から通知が届いた

※ランサムウェア攻撃： 組織の内部ネットワークに侵入した後、情報窃取やファイルの暗号化により、身代金の要求などを行う攻撃

このような攻撃を受けた場合は、情報セキュリティ事故の対応ルールに従うとともに、インシデント対応を進める上で、以下の情報も参考としてください。

「侵入型ランサムウェア攻撃を受けたら読むFAQ」

URL： https://www.jpcert.or.jp/magazine/security/ransom-faq.html
出所： 一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)